Believe in children
Barnardo's

Submission to Information Commissioner Age Appropriate Design Code Consultation
May 2018
Mihalis Papamichail, Policy and Research Officer
[redacted]

About Barnardo's

1. Barnardo's is the UK's largest children's charity supporting over 301,100 children, young people, parents and carers through over 1,000 services across the UK. Our services provide counselling for children who have been exploited, support for children in and leaving care and specialist mental health services. Barnardo's purpose is to transform the lives of the most vulnerable children and young people. We work to build stronger families, safer childhoods and positive futures for children and their parents and carers through our services, campaigns and research.

Overview

2. We welcome the Information Commissioner's draft Age Appropriate Design Code. However, we believe that the Code should make explicit reference to **vulnerable children** who have additional needs and life challenges (such as: young carers, children involved in gangs, care leavers). Barnardo's practitioners highlight that vulnerable groups of children may be more susceptible to online harms than other children. Insight from our services suggests that vulnerable children may find it particularly difficult to critically examine what they see and read online. This means that techniques and tools such as 'nudging' and 'profiling' could be impacting the decision making of vulnerable children differently.

   In responding to this consultation we have answered the questions which we have the most evidence on from our services.

Summary of recommendations

- The Code should give more attention to vulnerable groups of children with additional needs and life challenges (such as children with special needs and young carers).
- The Code should clarify whether geolocation tracking will automatically be switched off after a child has finished using a geolocation service.
- Geolocation data that is collected should only be used for purposes which child users are aware of.
- The Code must ensure that profiling of children (which has potential to cause harm) should be limited.

- It would be useful for the Code to provide additional examples of nudge techniques. (eg nudge techniques used in gaming or in encouraging children to pay for a certain product

Comments on the summary provisions

Best interests of the child

3. Article 3 of the UNCRC is central to the Code and Barnardo's greatly welcomes that this is a key component.

Age Appropriate Application

4. The different needs of children at different ages and stages of development should be at the core of how services are designed and Barnardo's are pleased to see that this is included as one of the provisions. In particular, for organisations that are not able to (or do not want to) verify which users are children, this Code must be applied to all users. This ensures that every child will be covered by the Code and Barnardo's greatly welcomes this.

5. Recent insight from our services[1] indicates that even children under the age of 5 are accessing social media, with many children under the age of 13 with a social media account. Our practitioners and the children that we work with highlight that young children should not be able to have a social media account. We therefore welcome the ICO's inclusion of an approach within the Code which limits age barriers and incentives for children to lie about their age.

Recommendation

- **This provision appears to focus predominantly on age and age verification. It does not, however, give sufficient attention to the fact that some children may have the requisite age but not the ability to understand, process and critically assess what they encounter online, such as children with special needs. The Code highlights that '*the standards must…take account the age and development needs of those children, to ensure appropriate protection for children of all ages*'. However, there is a lack of focus on development needs of particular children which need to be taken into consideration.**

[1] As highlighted in our forthcoming report: Left to their own devices: Young people, social media and mental health.

Transparency

6. Privacy information provided to users should be concise, prominent and in clear language suited to the age of the child and we commend the ICO for including this point in their draft guidance.

Recommendation

- **Nevertheless, the Transparency provision does not give enough attention to vulnerable groups of children with additional needs and life challenges. It is crucial that vulnerable children (such as children with special needs and young carers) are included within this provision. They must be able to access and understand information provided by a particular service.**

Default Settings

7. Barnardo's welcomes that the Code makes clear that 'settings must be high privacy by default' and that children's personal data will only be visible or accessible to other users of the service when the child amends their settings to allow this. This is something that the children and young people that we work with have called for. One of the children we work with for example recently asked: *'could it [social media access] be private by default?*

8. Without high privacy default settings, children can more easily be contacted by strangers online. Our practitioners have told us that young people are increasingly receiving friend requests from people they don't know. They also felt that many children (younger children in particular) don't know how to make their accounts private, or how to safeguard themselves from strangers.

9. The ICO's default settings provision means that, by default, companies should not make users' personal data visible to indefinite numbers of other users of the online service. At Barnardo's, we feel that this is a significant step forward.

Recommendation

- **Information about default setting should be in language that all children of all ages and development stages should understand.**

Geolocation

10. Barnardo's services support thousands of children that have experienced both online and physical sexual abuse and exploitation. In many cases our evidence suggests that online grooming can result in physical contact abuse. Information from our Child Sexual Abuse Services highlights that 2 in 3 of the children in this service were groomed online

before they were physically sexually assaulted. Data from our services also highlights that grooming can take place within 10 minutes of an online interaction.
As highlighted in our 'Digital Dangers[2]' report, technology enables perpetrators to more easily access children. As a child's location may be visible to other users, there is therefore the concern that geolocation technology, in particular, can put children's physical safety at risk (eg putting them at risk of sexual exploitation) by allowing perpetrators to access the physical location of a child. One of our services also told us that in some cases the families of children in care have been able to use geolocation technology to locate them and approach them inappropriately.

11. The Code states that 'settings which make the child's location visible to others revert to off after each use'. We are pleased to see that this is included within the Code and this is a welcome step to ensuring that a child's physical safety is not compromised. We equally welcome the fact that the Code intends to inform child users of when their location is being tracked.

12. Many of Barnardo's practitioners pointed out that **vulnerable children** (eg looked after children, young carers and care leavers) were more susceptible to the negative impacts of social media as they were more likely to experience isolation from friends and family, or struggle to develop and maintain these relationships offline due to the possible transient or unsettled nature of their life. Our Digital Dangers[3] report details how children with certain vulnerabilities appear to be particularly susceptible to online risks. This is partly due to seeking social interaction online that they are not able to achieve offline.

Recommendations

- **Although the Code makes clear that children have to change default settings to allow geolocation data to be used, it is not clear whether tracking will automatically be switched off after a child has finished using a geolocation service. The Code should therefore seek to clarify this.**

- **We recognise that geolocation can often be beneficial to children and can be used in their best interests (eg to reach places safely using map apps). However, geolocation data that is collected should only be used for purposes which child users are aware of. In other words, if a child is using geolocation technology when using a map, for example, geolocation data should not be used or gathered for any other purpose.**

Profiling

13. At Barnardo's we know that children can be exposed to harmful content online. The very nature of profiling algorithms, which are used to suggest content that users may

[2]Palmer, T Digital Dangers: The impact of technology on the sexual abuse and exploitation of children and young people http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf
[3] ibid

like, means that some children may be sent down a path of negative or harmful content that may be detrimental to their mental health and wellbeing.

Recommendation

- **We welcome the ICO's decision to include profiling within the Code. The Code states that services should 'switch options which use profiling off by default'. At Barnardo's, we are of the opinion that this does not go far enough to protect children from harmful content through profiling. Indeed, switching options off by default is much welcomed, however the Code must ensure that profiling (which has potential to cause harm) should be restricted in general.** [4]

Parental Controls

14. We endorse the ICO's inclusion of parental controls within the Code. Insight from our services indicates that young children may be exposed to online harms (for example they may be groomed or exposed to inappropriate content) without realising the dangers. Often parents and carers are not aware of their children's online interaction. At the same time we must not restrict the rights of children. In respect of this the Code provides a fair balance between protecting children from risk and allowing their right to privacy.

Recommendation

- **One of the key points raised by our services is that parents and carers are often not familiar with the type of risks that children can be exposed to. Our practitioners, as well as the children and young people that we work with, make clear that parents and carers must be educated on the positive and negative impacts of digital technology. It is perhaps beyond the scope of the Code to cover guidance and education for parents and carers on online risks, however, it could be highlighted that parental controls are only useful if parents and carers understand online risks.**

Nudge techniques

15. We commend the ICO for including nudge techniques in the Code. Any technique which unduly influences children to make choices that they wouldn't normally knowingly intend to make, should not be permitted. Nudge techniques also encourage user engagement, which can often lead to excessive use. Research suggests that there is a link between social media use and mental health and wellbeing.[5] Techniques which lead

[4] We understand that profiling does not always lead children to harmful content but can lead them to positive content also.

[5] See for example Understanding Society (2018) *Factors affecting children's mental health over time* Barardo's and the Children's Society https://www.understandingsociety.ac.uk/sites/default/files/downloads/general/understanding_society_mental_health_briefing_april2018_final.pdf

to excessive use among children can therefore be impacting on their mental health and wellbeing. One of our practitioners told us that:

' Excessive use means children are not doing other stuff like sport or reading, they describe feeling low and isolated but are online most of their free time. This often is in their bedroom at home alone.'

Recommendation

- **The Code provides two graphic examples of nudge techniques, however, there are other techniques used to influence a child's decision making that are not mentioned in the Code. It would be useful to provide additional examples of nudge techniques. (eg nudge techniques used in gaming or in encouraging children to pay for a certain product). As highlighted in para 3 of our response, vulnerable children with additional needs and life challenges may experience digital technology differently from other children. It is crucial therefore that this is taken into consideration.**